

# RIGHT TRIANGLES WITH ALGEBRAIC SIDES AND ELLIPTIC CURVES OVER NUMBER FIELDS

E. GIRONDO, G. GONZÁLEZ-DIEZ, E. GONZÁLEZ-JIMÉNEZ,  
R. STEUDING, J. STEUDING

**ABSTRACT.** Given any positive integer  $n$ , we prove the existence of infinitely many right triangles with area  $n$  and side lengths in certain number fields. This generalizes the famous congruent number problem. The proof allows the explicit construction of these triangles; for this purpose we find for any positive integer  $n$  an explicit cubic number field  $\mathbb{Q}(\lambda)$  (depending on  $n$ ) and an explicit point  $P_\lambda$  of infinite order in the Mordell-Weil group of the elliptic curve  $Y^2 = X^3 - n^2X$  over  $\mathbb{Q}(\lambda)$ .

## 1. CONGRUENT NUMBERS OVER THE RATIONALS

A positive integer  $n$  is called a congruent number if there exists a right triangle with rational sides and area equal to  $n$ , i.e., there exist  $a, b, c \in \mathbb{Q}^*$  with

$$a^2 + b^2 = c^2 \quad \text{and} \quad \frac{1}{2}ab = n. \quad (1)$$

It is easy to decide whether there is a right triangle of given area and integral sides (thanks to Euclid's characterization of the Pythagorean triples). The case of rational sides, known as the congruent number problem, is not completely understood. Fibonacci showed that 5 is a congruent number (since one may take  $a = \frac{3}{2}$ ,  $b = \frac{20}{3}$  and  $c = \frac{41}{6}$ ). Fermat found that 1, 2 and 3 are not congruent numbers. Hence, there is no perfect square amongst the congruent numbers since otherwise the corresponding rational triangle would be similar to one with area equal to 1. By the same reason one can restrict to square-free positive integers, a condition we will assume in the sequel.

There is a fruitful translation of the congruent number problem into the language of elliptic curves. Suppose  $n$  is a congruent number. It follows from (1) that there exist three squares in arithmetic progression of distance  $n$ , namely  $x - n, x, x + n$ , where  $x = c^2/4$ . Therefore their product  $(x - n)x(x + n)$  is again a rational square. In other words, a right triangle of area  $n$  and

---

*Date:* March 26, 2009.

*2000 Mathematics Subject Classification.* Primary 11G05; Secondary 11A99.

rational sides  $a, b, c$  corresponds to the rational point  $(c^2/4, c(a^2 - b^2)/8)$  on the elliptic curve

$$E_n : Y^2 = X^3 - n^2X.$$

Conversely, given a rational point  $(x, y)$  on  $E_n$  such that  $y \neq 0$ , one may define

$$a = \left| \frac{y}{x} \right|, \quad b = 2n \left| \frac{x}{y} \right|, \quad c = \frac{x^2 + n^2}{|y|} \quad (2)$$

to obtain a right triangle with rational sides  $a, b, c$  and area  $n$ .

Therefore,  $n$  is a congruent number if and only if the elliptic curve  $E_n$  has a rational point with non-vanishing  $y$ -coordinate. The correspondence between rational points on  $E_n$  and right triangles with rational sides and area  $n$  is not bijective. For instance, solving  $x$  and  $y$  with respect to  $a, b$  and  $c$  in equation (2) gives the two points

$$x = \frac{1}{2}a(a \pm c), \quad y = ax. \quad (3)$$

The points  $(x, y)$  with  $y \neq 0$  have infinite order in the Mordell-Weil group  $E_n(\mathbb{Q})$ , since it is known (see [6]) that the torsion subgroup of  $E_n(\mathbb{Q})$  consists only of points of order 2, that are  $(0, 0)$ ,  $(\pm n, 0)$ , and the point at infinity. From this one can deduce the fact, already known to Fermat, that there are in fact infinitely many right triangles with rational sides  $a, b, c$  verifying equation (1) for a given congruent number  $n$ , since scalar multiplication of the points corresponding to (3) on  $E_n$  yields new right triangles of area  $n$ .

Tunnell [8] found an intriguing approach towards the congruent number problem. He showed that if  $n$  is an odd square-free congruent number then

$$\begin{aligned} & \sharp\{x, y, z \in \mathbb{Z} : 2x^2 + y^2 + 8z^2 = n\} \\ &= 2\sharp\{x, y, z \in \mathbb{Z} : 2x^2 + y^2 + 32z^2 = n\}, \end{aligned}$$

and that the converse implication is also true provided the yet unsolved Birch & Swinnerton-Dyer conjecture holds (i.e., the rank of an elliptic curve  $E$  is positive if and only if the associated  $L$ -function vanishes at the central point:  $L(E, 1) = 0$ ). A similar criterion exists when  $n$  is even. This conjectural equivalent statement for the congruent number problem in terms of the number of representations of  $n$  by certain ternary quadratic forms allows to determine by computation whether a given integer  $n$  is congruent or not.

## 2. CONGRUENT NUMBERS OVER NUMBER FIELDS

A natural generalization of the congruent number problem is to allow the sides of the triangles to belong to an algebraic number field. The idea to

study the congruent number problem over algebraic extensions dates back at least to Tada [7] who considered real quadratic fields.

**Definition 1.** *Let  $\mathbb{K}$  be a number field and let  $n$  be a positive integer. We say that  $n$  is a  $\mathbb{K}$ -congruent number if there exist  $a, b, c \in \mathbb{K}$  such that (1) holds.*

Note that  $\mathbb{Q}$ -congruent numbers are nothing but the usual congruent numbers. When  $\mathbb{K}$  is a subfield of  $\mathbb{R}$  the geometric meaning still holds, since  $n$  being  $\mathbb{K}$ -congruent implies the existence of a right triangle with real sides in  $\mathbb{K}$  and area equal to  $n$ .

It is easy to see that any positive integer  $n$  is a congruent number for some quadratic extension of  $\mathbb{Q}$ . For instance,  $a = b = \sqrt{2}$  yields a right triangle with area equal to  $n = 1$ . However, equation (3) leads to the points  $(1 \pm \sqrt{2}, \sqrt{2} \pm 2)$  on the curve  $E_1$  which are all torsion points over  $\mathbb{Q}(\sqrt{2})$ . Therefore we do not get infinitely many different right triangles from these points. This example motivates the following definition:

**Definition 2.** *We say that a  $\mathbb{K}$ -congruent number  $n$  is properly  $\mathbb{K}$ -congruent if (1) has infinitely many solutions  $a, b, c \in \mathbb{K}$ .*

This definition is not interesting for  $\mathbb{K} = \mathbb{Q}$ , since all  $\mathbb{Q}$ -congruent numbers are properly  $\mathbb{Q}$ -congruent. But the example above shows that things may be different over number fields.

### 2.1. Congruent numbers over quadratic fields.

**Theorem 1.** *Every positive integer  $n$  is properly  $\mathbb{K}$ -congruent over some real quadratic field  $\mathbb{K}$ .*

**Proof.** Consider the system

$$\begin{cases} a^2 + b^2 = c^2, \\ ab = 2n. \end{cases}$$

Substituting  $a$  by  $2n/b$  in the first equation yields

$$4n^2 + b^4 = c^2 b^2.$$

Therefore

$$c = \frac{\sqrt{4n^2 + b^4}}{b}.$$

It follows that  $n$  is congruent over  $\mathbb{Q}(\sqrt{m})$ , where  $m = 4n^2 + b^4$  (and  $b$  is any chosen rational point).

Given such a triple  $(a, b, c) \in \mathbb{Q}(\sqrt{m})^3$ , the corresponding  $\mathbb{Q}(\sqrt{m})$ -rational point  $P$  on the curve  $E_n$  is given by (3). It is known (see [7, 4]) that the torsion subgroup of  $E_n(\mathbb{Q}(\sqrt{m}))$  reduces to the 2-torsion, namely  $\{\infty, (0, 0), (\pm n, 0)\}$ , except for the cases  $(n, m) = (1, 2)$  or  $(n, m) = (2, 2)$ .

We can choose  $b \in \mathbb{Q}$  such that  $m \neq 2$ , and therefore  $P$  is a non-torsion point. This finishes the proof.

**Remark 2.** Tada [7] showed that if  $n$  is not  $\mathbb{Q}$ -congruent, then it is congruent over  $\mathbb{Q}(\sqrt{m})$  if and only if  $nm$  is  $\mathbb{Q}$ -congruent. This fact has applications of the following kind.

Since it is known that 1 and 11 are not  $\mathbb{Q}$ -congruent numbers, it follows that 1 is not  $\mathbb{Q}(\sqrt{11})$ -congruent. According to the proof above,  $4n^2 + b^4 = 4 + b^4$  cannot be of the form  $11 \cdot d^2$  with  $d \in \mathbb{Q}$  for any choice of  $b \in \mathbb{Q}$ . That is, the genus 1 curve

$$11y^2 = x^4 + 4$$

is not an elliptic curve over  $\mathbb{Q}$ , i.e. it has no nonsingular  $\mathbb{Q}$ -rational point.

The same argument applied to a general pair  $n, m \in \mathbb{Z}^*$  leads to the following generalization. Denote by  $C_{n,m}$  the genus 1 curve  $C_{n,m} : my^2 = x^4 + 4n^2$ . Then this curve has a  $\mathbb{Q}$ -rational point if and only if  $n$  is  $\mathbb{Q}(\sqrt{m})$ -congruent, or equivalently, if and only if  $nm$  is  $\mathbb{Q}$ -congruent.

Note that the curve  $C_{n,m}$  is the twist by  $m$  of the curve  $C_{n,1} : y^2 = x^4 + 4n^2$ , that is another parametrization of the congruent number problem.

**2.2. Congruent numbers over cubic fields.** Next we shall construct an explicit non-torsion point on  $E_n$  over certain cubic fields (depending on  $n$ ).

**Theorem 3.** *Every positive integer  $n$  is properly congruent over some real cubic field. More precisely, for a positive integer  $n$  let  $\lambda = \lambda(n)$  be the unique real solution of the cubic equation*

$$32\lambda^3 - 32\lambda^2 + 8\lambda + n^2 = 0.$$

*Then the point  $P_\lambda = (x_\lambda, y_\lambda)$  with coordinates given by (6) and (7) below is of infinite order in the Mordell-Weil group of the elliptic curve  $Y^2 = X^3 - n^2X$  over  $\mathbb{Q}(\lambda)$ .*

**Proof.** We use an idea of Chahal [1]. Starting from an old identity of Desboves [2],

$$\begin{aligned} & (\mathcal{Y}^2 + 2\mathcal{X}\mathcal{Y} - \mathcal{X}^2)^4 + (2\mathcal{X}^3\mathcal{Y} + \mathcal{X}^2\mathcal{Y}^2)(2\mathcal{X} + 2\mathcal{Y})^4 \\ &= (\mathcal{X}^4 + \mathcal{Y}^4 + 10\mathcal{X}^2\mathcal{Y}^2 + 4\mathcal{X}\mathcal{Y}^3 + 12\mathcal{X}^3\mathcal{Y})^2, \end{aligned}$$

the substitution  $\mathcal{X} = 1 - 2\lambda, \mathcal{Y} = 4\lambda$  yields

$$\begin{aligned} & (1 - 12\lambda + 4\lambda^2)^4 + 8\lambda(2\lambda - 1)^2(2(1 + 2\lambda))^4 \\ &= (1 + 40\lambda - 104\lambda^2 + 160\lambda^3 + 16\lambda^4)^2. \end{aligned}$$

This gives the point  $(x, y)$  with coordinates

$$x = x(\lambda) = \frac{(1 - 12\lambda + 4\lambda^2)^2}{4(1 + 2\lambda)^2}, \quad (4)$$

$$y = y(\lambda) = \frac{(1 - 12\lambda + 4\lambda^2)(1 + 40\lambda - 104\lambda^2 + 160\lambda^3 + 16\lambda^4)}{8(1 + 2\lambda)^3} \quad (5)$$

on the elliptic curve  $y^2 = x^3 + dx$ , where  $d = d(\lambda) = 8\lambda(2\lambda - 1)^2$ . Now let  $n$  be a positive integer and consider the equation  $-n^2 = 8\lambda(2\lambda - 1)^2$ . It is easy to see that there is a unique real solution, explicitly given by

$$\lambda = \lambda(n) = \frac{1}{3} + \frac{1}{12}\kappa + \frac{1}{3\kappa},$$

where

$$\kappa = \kappa(n) = \sqrt[3]{-8 - 27n^2 + 3\sqrt{48n^2 + 81n^4}}.$$

Here we choose  $\kappa$  as the unique real third root which is negative for all  $n$ . By computation, we obtain a point  $P_\lambda = (x_\lambda, y_\lambda)$  on  $E_n(\mathbb{Q}(\lambda))$ , where the coordinates are given by

$$\begin{aligned} x = x_\lambda &= \frac{1}{4(n^2 - 16)^2} \{256 + 992n^2 + 65n^4 + (1024 - 2688n^2 - 28n^4)\lambda \\ &\quad + (1024 + 1920n^2 + 4n^4)\lambda^2\}, \end{aligned} \quad (6)$$

$$\begin{aligned} y = y_\lambda &= \frac{1}{32(n^2 - 16)^3} \{-16384 + 72704n^2 + 80960n^4 + 2868n^6 - n^8 \\ &\quad + (196608 - 462848n^2 - 145152n^4 - 1456n^6)\lambda \\ &\quad + (196608 + 421888n^2 + 100608n^4 + 208n^6)\lambda^2\}. \end{aligned} \quad (7)$$

This can be checked by use of a computer algebra package or by hand computation as follows: firstly, multiply the numerator and denominator of the coordinates (4) and (5) by the conjugates of  $(1 + 2\lambda)^2$  and  $(1 + 2\lambda)^3$ , respectively, then the coordinates are given as rational polynomials in the variable  $\lambda$ ; secondly, since  $\mathbb{Q}(\lambda)$  is a cubic field, these polynomials turn out to have degree at most two, which yields (6) and (7).

It remains to show that the point  $P_\lambda$  has infinite order on  $E_n(\mathbb{Q}(\lambda))$ . Note that the map that sends  $(x, y)$  to  $(-x, \sqrt{-1}y)$  is an endomorphism on the elliptic curve  $E_n$ , hence  $E_n$  has complex multiplication by  $\mathbb{Z}[\sqrt{-1}]$ . There are bounds [3, 5] for the order of the subgroup of torsion points on a elliptic curve with complex multiplication defined over a number field. Applying these results to the elliptic curve  $E_n$  over the cubic number field  $\mathbb{Q}(\lambda)$  we obtain that

if  $M$  is the order of a torsion point of  $E_n(\mathbb{Q}(\lambda))$ , then  $\phi(M) \leq 6$ , where  $\phi$  is Euler's  $\phi$ -function. Therefore  $M \in \mathcal{B} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 14, 18\}$ . Hence it is sufficient to prove that the order of  $P_\lambda$  is not in  $\mathcal{B}$ . For this purpose we use the  $m$ -division polynomial  $\Psi_m(x)$  associated with the elliptic curve  $E_n$ . It suffices to check that  $x_\lambda$  is not a root of  $\Psi_m(x)$  for  $m \in \mathcal{B}$  over  $\mathbb{Q}(\lambda)$ . We have

$$\Psi_m(x_\lambda) = P_{0,m}(n) + P_{1,m}(n)\lambda + P_{2,m}(n)\lambda^2,$$

where  $P_{k,m} \in \mathbb{Q}[n]$  has no integer roots for  $k = 0, 1, 2$  and  $m \in \mathcal{B}$ . Thus  $\Psi_m(x_\lambda) \neq 0$  for any integer  $n$  and  $m \in \mathcal{B}$ . This proves that  $P_{\lambda(n)}$  has infinite order and so the Mordell-Weil group of  $E_n(\mathbb{Q}(\lambda(n)))$  has positive rank. The theorem is proved.

**2.2.1. An example.** The integer  $n = 1$  is a congruent number over the cubic field  $\mathbb{Q}(\alpha)$ , where

$$\alpha = \frac{1}{3} + \frac{1}{12} \sqrt[3]{-35 + 3\sqrt{129}} + \frac{1}{3 \sqrt[3]{-35 + 3\sqrt{129}}}.$$

The following picture shows a right triangle with area 1 and sides in  $\mathbb{Q}(\alpha)$ :

$$\begin{array}{c} \frac{138\,048}{62\,195} + \frac{151\,008\,\alpha}{62\,195} - \frac{380\,736\,\alpha^2}{62\,195} \end{array} \quad \begin{array}{c} \text{1} \end{array} \quad \begin{array}{c} \frac{15\,817\,675}{6\,642\,426} + \frac{5\,151\,011\,\alpha}{3\,321\,213} - \frac{76\,896\,448\,\alpha^2}{16\,606\,065} \\ \frac{779}{890} - \frac{1879\,\alpha}{1335} + \frac{3776\,\alpha^2}{1335} \end{array}$$

We conclude with an interesting but difficult question:

*Given a number field  $\mathbb{K}$ , what are the congruent numbers over  $\mathbb{K}$ ?*

**Acknowledgements.** We thank J. Lehnert (Frankfurt) for useful discussions and P. Müller (Würzburg) for providing an alternative argument for Theorem 3. We also thank the referee for careful reading of the first version of this article and for pointing out some inaccuracies.

The fourth and the fifth author wish to thank the organizers of the 18th Czech and Slovak International Conference on Number Theory at Smolenice, August 27-31, 2007, for their kind hospitality and support.

Research of the third author was supported in part by grant MTM 2006-10548 (Ministerio de Educación y Ciencia, Spain) and CCG06-UAM/ESP-0477 (Universidad Autónoma de Madrid - Comunidad de Madrid, Spain). Research of the rest of authors was supported in part by grant MTM 2006-01859 (Ministerio de Educación y Ciencia, Spain).

#### REFERENCES

- [1] J.S. CHAHAL, Congruent numbers and elliptic curves, *American Mathematical Monthly* **113** (2006) 308–317.
- [2] A. DESBOVES, Sur l’emploi des identités algébriques dans la résolution, en nombres entiers, des équations d’un degré supérieur au second, *Comptes Rendus LXXXVII* (1879) 159–161, 321–322.
- [3] D. PRASAD AND C.S. YOGANANDA, Bounding the torsion in CM elliptic curves. *C. R. Math. Acad. Sci. Soc. R. Can.* **23** (2001), no. 1, 1–5.
- [4] S. KWON, Torsion subgroups of elliptic curves over quadratic extensions, *Journal of Number Theory* **62** (1997) 144–162.
- [5] A. SILVERBERG, Points of finite order on Abelian Varieties. *Contemp. Math.* **133**, 175–193 (1992).
- [6] J-H. SILVERMAN, The arithmetic of elliptic curves. *Graduate Texts in Mathematics*, 106. Springer-Verlag, New York, 1986.
- [7] M. TADA, Congruent numbers over real quadratic fields, *Hiroshima Math. J.* **31** (2001), 331–343.
- [8] J.B. TUNNELL, A classical Diophantine problem and modular forms of weight  $3/2$ , *Invent. Math.* **72** (1983), 323–334.

Ernesto Gironde  
Departamento de Matemáticas, CSIC  
Madrid, Spain  
ernesto.gironde@uam.es

Gabino González-Diez, Enrique González-Jiménez  
Departamento de Matemáticas, Universidad Autónoma de Madrid  
C. Universitaria de Cantoblanco, 28 049 Madrid, Spain  
gabino.gonzalez@uam.es, enrique.gonzalez.jimenez@uam.es

Rasa Steuding, Jörn Steuding  
Institut für Mathematik, Universität Würzburg  
Am Hubland, 97 218 Würzburg, Germany  
steuding@mathematik.uni-wuerzburg.de